Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-20 (canceled)

21. (Previously presented) A method for secure data transfer in a wireless networked communication system, the method comprising the acts of:

generating an encryption key within a first device of the communication system;

encoding the encryption key to form an encoded encryption key signal;

wirelessly transmitting the encoded encryption key signal to a second device of the communication system remote from the first device, wherein the first device and the second device are confined within a room and wherein the encryption key signal does not penetrate walls of the room;

decoding the encoded encryption key signal at the second device to extract the encryption key; and

using the encryption key to encrypt and decrypt conference data transmissions between the first and second devices, wherein the conference data transmissions are capable of penetrating the walls of the room.

22. (previously presented) The method of claim 21, wherein the encoded encryption key signal comprises an acoustic signal.

23. (previously presented) The method of claim 22, wherein the acoustic signal comprises DTMF tones.

24. (previously presented) The method of claim 21, wherein the encoded encryption key signal comprises an infrared signal.

25. (previously presented) The method of claim 21, wherein the act of decoding further comprises the act of storing the decoded encryption key in memory.

26. (previously presented) The method of claim 21, wherein the act of decoding further comprises the act of performing error detection to determine if an error has occurred in connection with the reception or decoding of the encryption key.

27. (previously presented) The method of claim 26, further comprising the act of sending a request for a retransmission of the encoded signal if an error is detected.

28. (previously presented) The method of claim 21, wherein the act of using the encryption key to encrypt and decrypt subsequent wireless transmissions further comprises the act of encoding the data into radio frequency signals.

29. (previously presented) The method of claim 21, further comprising the act of determining whether a new encryption key is required.

30. (Previously presented) A system for secure data transmission within a wireless communication system, comprising:

a first device of the communication system, the first device contained within a room and having an encryption key generator for generating an encryption key and a signal transmitter for wirelessly transmitting an encoded signal representative of the encryption key wherein the encryption key signal does not penetrate walls of a room; and

a second device of the communication system, the second device having a signal sensor for receiving the encoded signal from the first device and a decoder device for extracting the encryption key from the encoded signal, the encryption key being used to encrypt data being wirelessly transmitted between the first and second devices.

31. (previously presented) The system of claim 30 wherein the first device further comprises an encoder device for encoding the encryption key into an encoded encryption key signal for transmission.

32. (previously presented) The system of claim 31 wherein the encoder device comprises an acoustic codec.

33. (previously presented) The system of claim 30, wherein the encoded encryption key signal comprises an acoustic signal.

34. (previously presented) The system of claim 30, wherein the signal transmitter comprises an acoustic transmitter, and wherein the signal sensor comprises an acoustic sensor.

35. (previously presented) The system of claim 30, wherein the decoder device comprises an acoustic codec.

36. (previously presented) The system of claim 30 further comprising memory in the first and second devices for storage of the encryption key.

37. (previously presented) The system of claim 30 further comprising an encryption/decryption module in the first and second devices for encrypting data for transmission and decrypting data received from the other device.

38. (previously presented) The system of claim 30 further comprising a radio-frequency codec in the first and second devices for encoding the data into radio-frequency signals.

39. (previously presented) The system of claim 38 further comprising a radio-frequency transceiver in the first and second devices for transmission and reception of the radio-frequency signals within the communication system.

40. (previously presented) A system for secure data transmission within a wireless communication system, comprising:

means for generating an encryption key within a first device of the communication system;

means for encoding the encryption key to form an encoded encryption key signal;

means for wirelessly transmitting the encoded encryption key signal to a second device of the communication system remote from the first device, wherein the first device and the second device are confined within a room;

means for decoding the encoded encryption key signal at the second device to extract the encryption key; and

means for using the encryption key to encrypt and decrypt data for subsequent wireless transmissions between the first and second devices;

wherein the encoded encryption key signal_signal does not penetrate walls of the room containing the first device and the second device.